表１．情報家電の課題と解決の方向性

#	課題			解決の方向性	
	分類	小項目		対応項目	目標
1	脅威の共通認識 と セキュリティ対策 の 必要性	＜脅威＞ ・プラットフォームに汎用部品が使われてきており、任意コードの実行といった深刻な脅威も高まっている。 ・情報家電がネットワークアクセスを含め、PCの環境に近付いており、PCで起っている脅威と同等の脅威に晒される恐れがある。 ・製品の脆弱性対策を含めたアップデートには期間的な限界（プラットフォームのサポート期限等）があるが、家電の10～15年におよぶ長期間利用にどう対応していくか。		情報家電 セキュリティ基準	情報家電 セキュリティ基準 の確立
		＜業界の隘路・懸案＞ ・企業として、外部からくる脅威に対してまで、製品の安心、安全をどの程度、宣言できるのか。 ・情報セキュリティに起因した事故時、メーカーの責任範囲のコンセンサスが必要となる。 ・設定ミスなどもセキュリティの脅威になるため、マニュアル、取扱説明書の記載レベルの基準が必要である。			
		＜方向性： セキュリティ基準、ガイドライン、認証＞ ・業界で決めたセキュリティ対策上の基準的なものがあって初めて、ユーザも含めて不安が払拭される。 ・セキュリティ対策や脆弱性対応や暗号アルゴリズム選定のチェックリストや合意されたガイドラインが必要である。 ・中立機関による認証という仕掛けがあると望ましいが、極力コスト（認定期間含む）がかからない考慮が必要である。		認証・認定制度	
2	情報家電 市場形成 の必要性	＜ユーザ状況＞ ・安全との認識の強い家電において、起りうるセキュリティの脅威が一般消費者に理解して頂くのが困難である。 ・PCはセキュリティ対策が必須という市場形成がなされてきているが、情報家電のユーザー層はそれより広範となる。 ・情報家電に対するセキュリティ意識は行き渡っておらず、どう説明、理解してもらい、リテラシーの向上を図るかが課題である。 ・安全な筈の製品に何故セキュリティ対策でお金をかけるのか、なかなか理解が得られない。		ネット接続機能 利用で想定される脅威の理解	製品ライフサイクルへの対応 マーケットの育成（ベンダー）・リテラシーの向上（ユーザ）
		＜機器の利用面の隘路＞ ・取扱説明書には沢山書いてきているが、機器を正しく設定してもらえるかが課題である。 ・情報家電で何か起った時、どうすれば良いのか、機能利用だけでなくユーザのリテラシーの向上が重要である。		ユーザ意思による機能選定の認識	
		＜事故・故障対応＞ ・事故や故障の原因として、設定不良、ネット接続利用、改造や機能追加など様々考えられ、その切り分けが困難であり、またユーザとの責任分界点の明確化が必要である。 ・ユーザーは攻撃にあっていることや、自身が（踏み台等で）加害者になっていることに気付かないケースもある。		利用時（廃棄フェーズも含む）の留意事項の徹底	
		＜方向性： 市場形成＞ ・各社で個別にネット接続の注意事項、危険性をユーザに説明するのは難しく、業界で纏まったものが必要である。 ・製品品質と脆弱性は本質的に異なっており、脆弱性が原因でおきた事故をどう捉えるか、共通認識が必要である。		事故発生時の対応フローの整備・周知	
3	業界としての連携、 情報共有の必要性	＜業界としての連携＞ ・ネット接続に伴う危険性を各社が個別で出すのは難しく、業界で纏められることが望ましい。 ・脆弱性のレベルが軽微か、重大かの判断を各社がするのは難しく、共通の尺度が必要である		開発者向け情報DB	情報DBの整備
		＜情報共有の必要性＞ ・攻撃事例の共有、継続的に議論できる場や体制が必要である。 ・脅威情報、脆弱性情報など、業界で共有できるニュートラルなDBが必要である。 DBは、開発者向けと、ユーザー向けのそれぞれのものが必要である。		ユーザ向け情報DB	
4	市場の牽引 と発展	＜市場の牽引＞ ・世界市場でコスト、機能における競争の中で、コスト優先でセキュリティ対策レベルが低い情報家電が市場に出回るのは、ユーザにとっても、市場形成からも好ましくない。 ・海外OEM生産品の使用が増える方向であるので、それらにどのような受入れ検査をすればよいかも課題となる。		セキュリティ基準の国際標準化	グローバルデファクト・国際標準化への展開
		＜国際標準、認証＞ ・セキュリティ基準をISO等に提案して、それをクリアした、あるいは認証を受けた製品が消費者に選択される市場の流れを作るのが望ましい。		認証、認定制度の 市場デファクト化	